Computer Security & You

Virtual Program – August 2020

Whether you are using your computer to work, learn, or pass the time, we are on our home networks and devices more than ever. It is important to do what you can to keep you and your device secure at home.

What Lurks Out There

No matter what you call it, cybercrime can be a real pain. So it is good to understand the different kinds of crimes out there so you can be alert, protect yourself, and understand what might be going on if your computer or device starts acting weird.

Hacking: When someone breaks into a computer or network.

Malware: Any "malicious software" designed to secretly access your computer. Also known as viruses when it infects multiple locations.

Pharming: When website traffic is redirected to a bogus website, usually a shopping or banking site.

Spoofing: When cybercriminals try to get into your computer by masquerading as a trusted source. Examples include email spoofing (using email header that appears to be from someone you trust) and address bar spoofing (using malware to force you to view a specific web page).

Phishing: When cybercriminals try to get sensitive information from you, like credit card numbers and passwords. Some specific techniques include spear phishing (targets specific people), whale phishing (targets important people like CEOs), and SMiShing (phishing via text messages) and vishing (voice phishing that takes place over the phone, usually through impersonation).

How To Spot A Phishing Email

1. Watch for Overly Generic Content and Greetings

Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."

2. Examine the Entire Email Address

The first part of the email address may be legitimate, but the last part might be off by letter or may include a number in the usual domain.

3. Look for Urgency or Demanding Actions

"You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

4. Carefully Check All Links

Mouse over the link and see if the link destination matches where the email implies you will be taken.

5. Notice Misspellings, Incorrect Grammar, & Odd Phrasing

This might be a deliberate attempt to bypass spam filters.

6. Check for Secure Websites

Any webpage where you enter personal information should have a URL with https://. The "s" stands for secure.

Who Is the Culprit?

Online Criminals

Individuals who are really good at identifying what can be monetized, such as stealing and selling sensitive data or holding systems and information for ransom.

Foreign Governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way—perhaps to test their own skills or cause disruption for the sake of it.

Political Activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit an organization's activities.

Terrorists

Interested in spreading propaganda and disruption, they generally have less technical capabilities.

Malicious Insiders

Use their access to an organization's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest Mistakes

Sometimes staff, with the best of intentions, just make mistakes, such as emailing something sensitive to the wrong email address.

Is Everything A Scam?

Scamming is a multibillion-dollar business that drains people of their money, security, and privacy. Recent estimates indicate that users lose up to $36 billion annually. There are several common scams to be aware of.

Fake Sweepstakes or Lotteries

A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing often claiming that you have won a large sum of money or a prize.

Fake Ads

Fake pop-up advertising can include phone numbers to call, reputable brand names you recognize, and flashy gimmicks to attract your attention while you are surfing the internet. Avoid clicking on these ads that open in a

separate window, advertise free or heavily discounted products and services, and can potentially enable others to capture your personal information and/or maliciously steal your money.

Sweetheart Scams

Online dating is common practice in today's day and age to find romance. Be cautious of people who appear too good to be true, ask for personal information, or request money. Make sure you investigate the dating site before you create a profile.

Fake Credit Card Scams

There are many scammers out there trying to make a quick buck. Many will pose as credit card issuers suggesting that your personal information needs to be to gain access to your assets. Never give out personal information over the phone or in an email to people you do not know or have not called yourself.

What Can You Do?

Double-Check With Others

Never make unusual money transfers without talking to someone first. Criminals will rely on pressuring you in the moment and will do everything they can to ensure you do not talk to someone else! They will try to keep you engaged and imply a sense of urgency, thus giving you no time to think.

Play Hard To Get

Be stingy with your information. Never give away information on an impulse unless you are positive it is to a trusted source, such as a doctor or company you have done business with before. Cybercriminals use phishing tactics, hoping to fool their victims. If you are unsure who an email is from—even if the details appear accurate— or if the email looks "phishy,"

do not respond and do not click on any links or attachments found in that email. When available use the “junk” or “block” option to no longer receive messages from a particular sender.

Everybody Lies

If a deal on a vacation, prescription drug, or anything else seems too good to be true, it probably is. Research the company offering the deal. See if anyone has reported interacting with the company or the deal.

Don’t Fall For Bad Actors

If someone is trying to sell something to you or get more information out of you, ask for verification about who they represent. If they refuse, walk away or hang up the phone. If you are unsure about the information, look up the phone number of the organization and call them.

Government Loves The Postal Service

The U.S. government never uses email, website ads, or phone calls to notify you of an infraction or collect personal information from you. The government will always send you a letter in the mail to contact you. If you do receive a phone call claiming to be from the government, look up the number on your own instead of using what they give you.

Secure Your Devices

The smartphones, tablets, laptops, or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks using these preventive measures.

Keep It Updated

Do not ignore software updates as they contain patches that keep your device secure. If you are prompted to install any updates, consider that you take the time to do so.

Careful Downloading

Avoid downloading dodgy apps. Only use official app stores, like Google Play or the Apple App Store, which provide some protection from viruses. Do not download apps from unknown vendors and sources. If ratings and reviews are offered, take a look before downloading any unknown applications.

Lock It Down

Always lock your device when you are not using it. Use the PIN, password, fingerprint, or face id feature. This will make it harder for an attacker to exploit a device if it is left unlocked, is lost, or is stolen. Even if you live in a safe neighborhood, you probably lock your doors when you are not home. Do the same with your device. Why allow anyone the ability to access your digital life?

Disable Location Services

It should come as no surprise that tech companies use the location services on your smartphone to track your comings and goings. That is how they give you up-to-date traffic reports, restaurant recommendations, and other helpful information. But they also sell that information to marketers and other companies interested in studying your habits. Many apps have automatic location services. Make sure you are in control of who is trying to locate you. You can find these controls in your settings on your device where you can turn them off and on.

Back It Up

Data is the most important asset on your device. Computers and other devices can fail, get stolen or destroyed, and be subject to malware. Backing up your data can help prevent you from being powerless over your

data and can help protect and restore your data in case something goes wrong. For your most important data, consider doing one of the following:

• Make three copies of your data

• Store your data using two different media types or methods

• Store the backup device that holds your copied files in a safe place

Virus Protection

Antivirus software is designed to detect, prevent, and take action to disarm or remove malicious software from your computer. It may also prevent or remove unwanted spyware and adware. Antivirus software will begin by checking your computer programs and comparing them to known types of malware. It will also scan your computer for behaviors that may signal the presence of a new, unknown malware. Although the detection tools are highly effective, no antivirus software is perfect.

Best Free Antivirus Protection	**Best Paid Antivirus Protection**
Avast Free Antivirus	McAfee Antivirus Plus
Kaspersky Security Cloud Free	Kaspersky AntiVirus
AVG Antivirus Free	Bitdefender Antivirus Plus

Secure Yourself

Multiple Factor Authentication

Multiple factor and two-factor authentication add a strong extra layer of protection for your personal and financial data. Alongside your account username and password, you enter a one-off code received via call or text. By enabling multi-factor authentication, you are ensuring that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. It is recommended that any time multi-factor authentication is an option, enable it by using a trusted mobile device, such as your smartphone, an

authenticator app, or a secure token which is a small physical device that can hook onto your key ring.

Password Protocol

There is just too many passwords! And of course, it is recommended to use a different password for each account. So what can you do?

Password Management Tools

Use a password management tool if possible. Password managers generate and remember different, complex passwords for each of your accounts. No more struggling to come up with clever, cryptic passwords that you have a hard time remembering. With a secure and easy-to-use password manager, you can manage your login credentials across all your devices, keeping your passwords secure and automatically filling in forms. A password manager is essentially an encrypted digital vault that stores the login information you use to access apps, websites and other services. The free version of LastPass is one of the best password manager tools out there.

Unique Passwords

But if you need to create a password, here are a couple of recommendations. Combine upper and lowercase letters, numbers and symbols. Maybe create a special sentence, switching characters, numbers, or symbols for certain letters. You should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cybercriminals from gaining access to these accounts and protect you in the event of a breach. With all the recent news of security breaches and identity theft, using unique passwords can go a long way to ensuring that if one site gets hacked, your stolen password cannot be used on other sites.

Never Click and Tell

Social media can be a sinkhole of personal information. Limit what information you post on social media—from personal addresses, where you like to grab coffee, to when and where you are going on vacation. What many people do not realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and your physical belongings. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and relationships. Disable location services that allow anyone to see where you are – and where you are not – at any given time. Be frugal in what you share and how you share it.

Secure Sites and Apps

When visiting unknown websites, keep an eye out for a lock in the address bar. This lock means that the connection is secure and that your information is private when sent to the website. Be sure to look for this lock whenever you are entering information, such as names, addresses, and credit card numbers. Alternatively, websites that begin with “https://” are also safe, where the “s” stands for secure. In addition, most of the popular web browsers like Google Chrome, Safari, and Firefox will alert you when a website is not secure and is not offering you a safe connection. Avoid these websites, and never give them your personal or financial information.

Reporting Cyber Crime

More than 80 percent of online scams go unreported, partly because people do not know how or where to report them.

Banking and Retirement Fraud

Contact your bank or retirement facility immediately. Scams often involve money coming from bank or retirement accounts. As soon as you discover

that you or someone you know has been scammed, notify whomever deals with the account. You might still have a chance to recover money, or it might not have left the account yet.

Cyber Crime

The Internet Crime Complaint Center is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Complaints may be filed online. Keep in mind, you will need to contact your credit card company directly to notify them if you are disputing unauthorized charges on your card or if you suspect that your credit card number has been compromised.

Online Business/Shopping Scams

If you suspect a business is scamming you online, report it to the Better Business Bureau. A map on their website identifies businesses all over the country that have tried to scam people in person and on the web.

Phishing and Telemarketing Scams

The Federal Trade Commission shares consumer complaints covering a wide range of categories, including online scams, with local, state, federal, and foreign law enforcement partners. It cannot resolve individual complaints, but can give you information on the next steps to take.